

1-18-00

A

HEWLETT-PACKARD COMPANY

PATENT APPLICATION

Intellectual Property Administration
P.O. Box 272400
Fort Collins, Colorado 80528-9599

ATTORNEY DOCKET NO. 10980251-1

IN THE U.S. PATENT AND TRADEMARK OFFICE
Patent Application Transmittal Letter

ASSISTANT COMMISSIONER FOR PATENTS
Washington, D.C. 20231

Sir:

Transmitted herewith for filing under 37 CFR 1.53(b) is a(n): ☒ Utility ☐ Design☒ original patent application,☐ continuation-in-part application

jc542 U.S. PTO
09/483183
01/13/00

INVENTOR(S): Daniel R Tretter et al

TITLE: A Secure Network-Based System for the Distributed Printing of Documents

Enclosed are:

- ☒ The Declaration and Power of Attorney. ☒ signed ☐ unsigned or partially signed
☒ 5 sheets of drawings (one set) ☐ Associate Power of Attorney
☐ Form PTO-1449 ☐ Information Disclosure Statement and Form PTO-1449
☐ Priority document(s) ☐ (Other) _____ (fee \$ _____)

CLAIMS AS FILED BY OTHER THAN A SMALL ENTITY				
(1) FOR	(2) NUMBER FILED	(3) NUMBER EXTRA	(4) RATE	(5) TOTALS
TOTAL CLAIMS	23 — 20	3	X \$18	\$ 54
INDEPENDENT CLAIMS	4 — 3	1	X \$78	\$ 78
ANY MULTIPLE DEPENDENT CLAIMS	0		\$260	\$ 0
BASIC FEE: Design \$310.00); Utility \$690.00)				\$ 690
TOTAL FILING FEE				\$ 822
OTHER FEES				\$
TOTAL CHARGES TO DEPOSIT ACCOUNT				\$ 822

Charge \$ 822 to Deposit Account 08-2025. At any time during the pendency of this application, please charge any fees required or credit any over payment to Deposit Account 08-2025 pursuant to 37 CFR 1.25. Additionally please charge any fees to Deposit Account 08-2025 under 37 CFR 1.16, 1.17, 1.19, 1.20 and 1.21. A duplicate copy of this sheet is enclosed.

"Express Mail" label no. EL 187 270 222 USDate of Deposit Jan. 13, 2000

I hereby certify that this is being deposited with the United States Postal Service "Express Mail Post Office to Addressee" service under 37 CFR 1.10 on the date indicated above and is addressed to: Assistant Commissioner for Patents, Washington, D.C. 20231.

By Dee Timmons

Typed Name: Dee Timmons

Respectfully submitted,

Daniel R Tretter et al

By Timothy R Croll

Timothy R Croll

Attorney/Agent for Applicant(s)

Reg. No. 36,771

Date: Jan. 13, 2000

Telephone No.: (650) 857-4881

A SECURE NETWORK-BASED SYSTEM FOR THE DISTRIBUTED PRINTING OF DOCUMENTS

BACKGROUND OF THE INVENTION

5 The present invention relates to a computer-based system for distributing and printing electronic documents. The present invention also relates to electronic commerce over the Internet.

 Distributed computer systems such as the World Wide Web provide excellent vehicles for the timely dissemination of documents and images over
10 broad geographical areas. The Web allows documents and images to be shared among different people in different geographic regions.

 One scenario for a distributed computer system involves the sharing of documents between multiple corporate offices in different cities. The documents and images are stored in a central repository, where they can be
15 managed and updated easily. Users of the Web can access the repository and obtain desired hardcopies immediately. It is quite common for some corporations to restrict the distribution of certain sensitive documents. These documents are typically tagged with a serial number, and each numbered document can only be delivered to an authorized person. Thus, security -
20 protecting the documents from unauthorized use - is an important consideration to the successful implementation of such a system. Hence a system that provides the realization of distribute-and-print concept in a secure manner would be desirable.

 Another scenario for a distributed computer system involves electronic
25 commerce where, for example, a merchant sells valuable documents (e.g., out-of-print books, images of fine art) to a customer over the Internet. Not only is there a need for a secure way of delivering the documents and images over the Web, but there is also a need for a secure mechanism for controlling the number of hardcopies generated by the customer. In other words, a customer
30 should be allowed to print only the specified number of copies for which he or

she paid. Hence a secure printing system that provides a "pay-per-print" service would also be desirable.

5

SUMMARY OF THE INVENTION

According to one aspect of the present invention, a system for the distributed printing of a document includes a computer network, a server connected to the network, and a printer connected to the network. The document is stored on the server. The printer uses a cryptographic key to
10 establish an identity with the server via the network. After a document is ordered from the server via the network, the server encrypts the ordered document and places the encrypted document on the network. The printer retrieves the encrypted document from the network, decrypts the retrieved document, and prints the decrypted document.

15

The invention may be adapted for electronic commerce, in which a customer negotiates a document order via the Internet, and a document server sends the ordered documents to the printer. The printer then prints out high quality copies of the documents. However, the printer only prints the number of copies that is specified in the document order. Once the printing
20 has been completed, the customer is automatically charged according to the type and number of documents that are printed. More generally, however, the invention may be used to distribute documents in a secure manner to authorized users on an unsecure network.

20

Other aspects and advantages of the present invention will become
25 apparent from the following detailed description, taken in conjunction with the accompanying drawings, illustrating by way of example the principles of the invention.

30

BRIEF DESCRIPTION OF THE DRAWINGS

Figure 1 is an illustration of a secure Internet-based system for the distributed printing of documents;

Figure 2 is an illustration of a client-server communication during a commercial transaction;

5 Figures 3a and 3b are illustrations of a printer-server communication during the commercial transaction;

Figure 4 is an illustration of an alternative client-server communication during the commercial transaction;

10 Figure 5 is an illustration of a client-server communication during a non-commercial transaction; and

Figure 6 is an illustration of a smart card for the system.

DETAILED DESCRIPTION OF THE INVENTION

15 As shown in the drawings for purposes of illustration, the present invention is embodied in a system that allows an authorized user to select and generate hardcopies of documents in a secure, controlled manner. Security of the system is realized by an aggregate of a secure communication protocol, smart card technology and the computational infeasibility of breaking a
20 cryptographic system. The documents may be distributed over the Internet. Therefore, document orders may be placed from any location having access to the Internet. The system may be used for electronic commerce, in which copies are made on a "pay-per-print" basis.

Reference is made to Figure 1, which illustrates a secure system 10 for
25 the distributed printing of documents. The system 10 includes a computer network 12 and a server 14 connected to the network 12. The network 12 is not limited to any particular type. To simplify the explanation of the invention, the system 10 will be described in connection with a network 12 including the Internet 12a and a local area network ("LAN") 12b that is connected to the
30 Internet 12a.

The server 14 hosts a web site for distributing documents over the Internet 12a. The documents can be distributed to any client that can connect to the Internet 12a and access the web site. The server 14 includes a processor 16, memory 18 and a network interface 20. Stored in the server
5 memory 18 are web page content 22 and a repository 24 of documents. The web page content 22 allows a client to place an order for one or more documents in the repository 24. A document may include material that contains text, images, and graphics. Also stored in the server memory 18 are an operating system 26 and a server program 28, both of which are executed
10 during operation of the server 14. An HTTP daemon, the server program 28 runs on top of the operating system 26. The server program 28 allows the server 14 to communicate with clients connected to the Internet 12a. For example, the server program 28 can run an interface program 30 such as a CGI program or a Java applet in response to document orders and other client
15 requests received from the Internet 12a. The interface program 30 allows the server 14 to receive document orders from clients via the Internet 12a and respond to the document orders by performing secure document distribution as described below in connection with Figures 3a and 3b.

Any number of clients can connect to the Internet 12a, log onto the web
20 site and place document orders with the server 14. The clients may be any types of machines that can communicate over the Internet (e.g., personal computers, work stations, Personal Digital Assistants, Java appliances). Only two clients 32 and 34 are shown to simplify the explanation of the invention. A first client 32 is connected to the Internet 12a via the LAN 12b, and a second
25 client 34 is connected directly to the Internet 12a. For example, the first client 32 may be a personal computer having web browser software.

A secure printer 36 is also connected to the Internet 12a via the LAN 12b. The printer 36 is not limited to any particular type. For instance, the printer 36 may be a laser printer or an ink jet printer. The printer 36 includes a
30 smart card reader 38 and an electronics assembly. The electronics assembly,

in turn, includes an Application Specific Circuit ("ASIC") having an embedded processor 40, read-only memory ("ROM") 42 and random access memory ("RAM") 44. The embedded processor 40 can communicate with the smart card reader 38, the ROM 42 and the RAM 44. Stored in the ROM 44 is a program 46 for instructing the embedded processor 40 to operate the printer 36 and communicate with the server 14 to perform secure document distribution as described below.

A smart card 48 such as a PCMCIA card may be inserted into the smart card reader 38 of the secure printer 36. The smart card 48 stores a unique cryptographic key or key pair, depending upon the type of cryptographic algorithm that is used.

Public or private key algorithms may be used. If a public key algorithm such as RSA is used, a key pair consisting of a public key K_A and a private key K_B is generated and stored in the smart card 48. The public key K_A is used to encrypt a message M to produce an encrypted message U , and the private key K_B is used to decrypt the message U . Thus, $U = E_{K_A}(M)$, where $E_{K_A}(\bullet)$ denotes the encryption operation with key K_A ; and $M = D_{K_B}(U)$, where $D_{K_B}(\bullet)$ denotes the decryption operation with the private key K_B . Computational feasibility of breaking the encrypted message depends in part upon key length.

If a private key algorithm such as DES is used, a single session key K_S is generated. The DES key K_S is symmetric, that is, it is used for both encryption and decryption. Thus, $U = E_{K_S}(M)$ and $M = D_{K_S}(U)$. Private key encryption and decryption are generally faster to perform than public key encryption and decryption.

Figures 2, 3a and 3b illustrate a commercial transaction between a customer and the server 14. The commercial transaction is a "pay-per-print" transaction. The customer contacts a document vendor and places an order specifying a document and a number of copies. The server 14 delivers the specified document to the secure printer 36, and the secure printer 36 prints

out the specified number of copies. Figure 2 illustrates communication between the customer and the server 14; and Figures 3a and 3b illustrate communication between the server 14 and the secure printer 36.

Before the first commercial transaction is initiated, the customer gains
5 access to the secure printer 36 and a smart card 48. The secure printer 36 might be located in the same room as the customer. The smart card 48 may be issued by the owner of the web site or it may be obtained from a third party such as a party maintaining the web site or a trusted certificate authority.

By way of example, public key encryption and decryption will be
10 performed during the course of the transaction. Therefore, the smart card stores a key pair consisting of a public key KA and a private key KB.

Referring first to Figure 2, the customer initiates the transaction by logging onto the web site of the document vendor (block 102). The customer may run a web browser on the first client 32 to log onto the web site. The
15 customer enters the URL of the document vendor's web site and downloads different files from the server 14. The files cause the first client 32 to display the document vendor's web page. The web page advertises the vendor's documents in the repository 24 and allows the customer to order the documents. The document vendor may choose any number of ways to
20 advertise the documents in the repository 24. Documents may be advertised by title and author lists. Abstracts and thumbnail images of the documents may also be provided.

The server 14 allows the customer to preview the documents (block 104). For example, the server 14 allows the customer to download low quality
25 images of the documents. The low quality images may contain incomplete text (e.g., a title and synopsis) and low-resolution images that are visibly watermarked. Consequently, the preview process does not compromise the value of a high quality document. The preview/selection process discourages the customer from simply printing the preview document on the screen and,

hence, obtaining it without payment because hardcopies of the preview images are of visually low quality.

To protect the integrity of visibly watermarked images, an authentication watermark may also be inserted (it is relatively easy for anyone
5 to insert a logo of a company into an image and then claims that the image was originated from that company). In that way, the customer can verify whether the received preview images are authentic.

The customer places an order by selecting the advertised documents and specifying the number of copies of each document (block 106). The
10 documents may be ordered and selected in many different ways according to the design of the server 14 and the customer model. For example, after previewing the documents, the customer enters selected documents in an electronic form. The customer also specifies the number of copies of each document in the form. The form already establishes the price for each
15 document. The customer also enters a form a payment. For example, the customer might provide a credit card number, or perhaps charge an existing account with the vendor. Once filled, the form is sent to the interface (e.g., CGI) program 30 of the server 14. Although more than one document may be selected, the transaction will be described for only a single document.

20 Before the order can be carried out, the customer is asked to identify the secure printer 36 to which the documents will be delivered (block 108). This will allow the server 14 to communicate with the secure printer 36. If the secure printer 36 has a URL, the customer may enter the URL of the secure printer 36.

25 After the order has been placed and the printer identified, the customer then inserts the smart card 48 into the card reader 38 of the secure printer 36 (block 110). The secure printer 36 becomes active and communicates with the server as described below in connection with Figures 3a and 3b.

If the order goes through, the server sends the document to the secure
30 printer 36, and the secure printer 36 prints out the document in the number

specified in the order. The customer then retrieves the copy or copies from the secure printer 36 (block 112). The transaction is finished.

Reference is now made to Figures 3a and 3b, which illustrate the communication between the server 14 and the secure printer 36 during the commercial transaction. After the secure printer 36 has been identified, the server 14 establishes a connection with the secure printer 36 (block 202). The connection is established via the Internet 12a. The server 14 then waits for the customer to insert the smart card 48 in the secure printer 36 (block 204). If the smart card 48 is not inserted within a predetermined amount of time, the server 14 time outs, closes the connection with the secure printer 36 and cancels the document order (block 206).

When customer inserts the smart card 48 into the card reader 38, the printer 36 becomes active, and reads the key pair KA and KB from the smart card 48 (block 208). In this manner, the printer 36 takes on the identity of the smart card 48.

If the server 14 has not timed out, the secure printer 36 then establishes its identity with the server 14 by sending the public key KA to the server 14 (block 210). The server 14 verifies that the public key KA is a valid smart card key (block 212). For example, the server 14 can verify the public key KA by sending the public key KA to a trusted central location that associates public keys with users, or the server 14 can look up a local list of all registered users.

Once the public key KA has been verified as a valid smart card key, the server 14 proceeds to authenticate the identity of the smart card 48 and, therefore, the secure printer 36. To authenticate the identity of the secure printer 36, the server 14 generates a unique session token T and encrypts it using the public key KA (block 214). Thus, $U = E_{KA}(T)$, where U is the encrypted token. The session token T may be an arbitrary message. The encrypted token U is sent to the printer 36 via the Internet 12a (block 216).

The secure printer 36 uses the private key KB to decrypt the encrypted token U (block 218). Thus, $T' = E_{KB}(U)$. The secure printer 36 sends the decrypted token T' back to the server 14 for verification (block 220). Since only the smart card 48 and printer 36 should store the private key KB , only the printer 36 should be able to decrypt the message to produce the decrypted token T' . Thus, the server 14 verifies that the printer 36 has the identity of the smart card 48 if $T = T'$ (block 222). At this stage, the identity of secure printer 36 has been authenticated. The authentication is performed because the list of all public keys is available as public information. It discourages any unauthorized user from implementing a device in software and/or hardware to falsely claim the identity of the smart card 48.

After the identity of the secure printer 36 has been authenticated, the server 14 accesses the file X of the ordered document from the repository 24 (block 224). The server 14 also concatenates a word to the file X , the word representing the number of copies of each document that has been ordered (block 226). This word may be inserted at the beginning of the file X or appended to the end of the file X .

The server 14 then encrypts the file X (block 228). Resulting is an encrypted message $U1$. Encryption is performed by using the public key KA . Thus, $U1 = E_{KA}(X)$.

The encrypted message $U1$ is then transmitted to the secure printer 36 (block 230). Even if the data transmission is intercepted, an eavesdropper will not be able to generate high quality copies without knowing the decryption key KB .

The secure printer 36 receives the encrypted message $U1$ as a bit stream and decrypts the encrypted message $U1$ using the private decryption key KB (block 232). Resulting is a decrypted document X' . Thus, $X' = D_{KB}(U1)$.

The secure printer 36 parses the word representing the number of copies and prints the specified number of copies of the decrypted document X'

(block 234). Since decryption is performed within the secure printer 36, the customer is prevented from redirecting the decrypted document X' to an ordinary printer and generating any number of hardcopies there. Since the word representing the number of copies is encrypted, the copy number cannot
5 be changed either. Consequently, the secure printer 36 will only print the number of copies of the document specified in the document order.

The printer 36 monitors its own actions to verify that the document has printed successfully. After the printing is completed, the printer 36 sends an acknowledgment to the server 14 to indicate that the required printing has
10 been performed (block 236). The server 14 then logs the transaction. This triggers a billing process in which the customer's account is charged for the copies that were actually printed (block 238). If the secure printer 36 becomes jammed and does not print out all of the ordered copies, the customer will only be charged for the number of copies that were actually
15 printed.

The form of the document that is encrypted will depend upon how and where document rendering is performed. Document rendering is preferably performed inside the secure printer 36 so that the rendered data cannot be diverted to a non-secure printer (rendered data could be diverted if rendering
20 is performed in a software module in a host computer and the printer simply performs the physical task of putting dots on paper according to the result produced by the host software).

The secure printer 36 renders the document to generate high quality hardcopies by performing steps such as scaling, color correction, and half
25 toning. Since the characteristics of various printers vary a great deal, the optimum half toning method depends on a variety of printer parameters such as print resolution.

Depending upon how the document is created, the optimum rendering strategy might also be different. A typical document can contain various
30 combinations of text, images, and graphics. The optimum rendering algorithm

for each of these objects (text, images, or graphics) is typically distinct. For example, graphics may be best rendered with vivid color (i.e., high saturation) and scattered-dot halftone. Images, on the other hand, may be rendered with screen-matching color and perhaps adaptive type of half toning. If the document was generated by, for example, a word processor, then the resulting file typically contains information on the various types of data in different areas within the page. Hence the optimum rendering strategy may be applied accordingly.

In a different scenario where the document is digitally scanned in from existing hardcopy archives, a segmentation algorithm may be performed to separate out the text, images, and graphics regions. The same data dependent rendering methods can then be applied.

Thus disclosed is a system that allows an authorized user to select and generate hardcopies of documents in a secure, controlled manner. Security of the system is realized by an aggregate of a secure communication protocol, smart card technology and the computational infeasibility of breaking a cryptographic system.

The system offers various countermeasures against attack. An unauthorized number of copies cannot be printed because the number is encrypted along with document. It is not accessible to user.

If a preview document is printed, the printed text will be incomplete, and the printed images will be of low quality. Preview images cannot be intercepted and corrupted because authentication watermarks make substitution detectable by user.

Even if a document from server is intercepted, the document will be encrypted. Without the decryption key, reproducing the intercepted document will be extremely difficult.

Even if the secure printer is emulated in software on another machine, the decryption keys are not available to the emulator. Therefore, the token cannot be decrypted and the emulator will not be authenticated.

The system monitors and acknowledges the printing operation. Therefore customer only pays for what is printed out.

The system may be used to implement a "pay-per-print" service for documents, where a document owner can sell documents over the Internet.

- 5 The secure printing system can be useful in many business applications. One example is the trading of valuable documents or images, where a user accesses the document server through the World Wide Web and then purchases and generates hardcopies using a secure printer. The images would be of high quality, and the printer would be of such a type that can
- 10 reproduce the high quality images (e.g., museum posters, brochures). The system may be used to distribute reprints from magazine articles, books that are out-of-print, and it may be used at a college bookstore to distribute course packets.

- The invention is not limited to the specific embodiments described and
- 15 illustrated above. Ordering a document and distributing the document may be performed on different channels. Referring to Figure 4, the customer calls the vendor over a telephone, places an order for a document, and supplies credit card information (block 302). The customer also identifies a location of a secure printer 36 to which the customer has access (block 304). The location
- 20 identifier may be an address other than a URL. After the order has been placed, the customer inserts a smart card into the identified secure printer 36 (block 306) and retrieves the documents that have been printed out (block 308). The printer 36 and server 14 may communicate as illustrated in Figures 3a and 3b.

- 25 The invention is not limited to electronic commerce. The invention may be used more generally to distribute documents in a secure manner to authorized users on an unsecure system, regardless of whether the users are charged for the documents.

- In a corporate setting, for example, an employee might place a call to
- 30 human resources in order to access personal records. Referring to Figure 5,

the employee gives an employee ID, pin number or some other access code (block 402) and identifies a secure printer to which the documents will be delivered (block 404). If the secure printer is connected to a local server via a local area network, the employee might identify the secure printer by printer
5 number. The employee then inserts the smart card in the identified printer (block 406) and retrieves the documents that are printed out. The printer and server may communicate as illustrated in Figures 3a and 3b, except that the customer is not charged for the printed documents.

The smart card is not limited to a PCMCIA card. For example, the
10 smart card may be a laminated plastic card having a magnetic strip for storing the cryptographic key(s).

Private key encryption may be used in conjunction with public key encryption. For instance, a secure printer randomly generates a unique session key KS that is used for encryption and decryption of the selected
15 documents. The session key KS is encrypted with a public key of the server and sent to the server. The server decrypts the session key with its private key. The server later encrypts the selected documents using the session key and transmits the encrypted document to the printer. The printer then uses the session key to decrypt the document. Thus, decryption and printing are
20 performed in the same way as before, except that the private key cryptographic system is used in combination with the public key cryptographic system.

In an alternative implementation, the server could generate the random session key and encode it along with the session token. Then, in addition to
25 decrypting the session token and sending it back to the server for verification, the printer would also decrypt the session key KS which, in turn, will be used to decrypt the encrypted documents. This alternative implementation can reduce the total number of printer—server communications performed during a session.

30 Instead of using a computer to preview and select documents, this

functionality can be integrated into the secure printer. Resulting is a standalone client machine. Such a printer may run a Java Virtual Machine, and it may include a keypad for entering the URL of the web site on the document server and a simple display for allowing a customer to preview and
5 select documents. Such an integrated approach is appropriate if the client is set up as a printing kiosk or dedicated system.

The cryptographic key(s) may be embedded in the ROM of the printer. Thus, the printer becomes trusted, not the holder of the smart card.

The smart card may perform decryption instead of the printer.
10 Referring to Figure 6, a smart card 500 such as a PCMCIA card includes an embedded processor 502 and store an encryption algorithm 504 and at least one encryption key 508 in ROM 506. The decryption is performed entirely within the smart card 500. Results would be passed to the printer. Thus, the printer passes the encrypted token and document from the network to the
15 smart card, and the smart card passes the decrypted token and document to the printer. An advantage of performing the decryption entirely within the smart card 500 is that the private decryption key never needs to be revealed outside of the smart card. This adds another level of security to the system. Moreover, having the smart card 500 perform decryption unloads some
20 computational burden from the secure printer.

Accordingly, the invention is not limited to the specific embodiments described and illustrated above. Instead, the invention is construed according to the claims that follow.

WHAT IS CLAIMED IS:

1. A method of using a printer to distribute a document stored on a server, the server being connected to a network, the method comprising the steps of:

- 5 using the printer and at least one cryptographic key to establish a printer identity with the server;
- using the printer to receive an encrypted document from the network;
- using the printer to decrypt the document; and
- using the printer to print the decrypted document.

2. The method of claim 1, wherein the encrypted document includes a message indicating a number of copies to be printed; and wherein the printer prints the number of document copies indicated in the message.

3. The method of claim 1, wherein the printer includes a smart card reader; and wherein the printer identity is established by inserting a smart card into the reader.

4. The method of claim 3, wherein the smart card is used to perform the decryption.

5. The method of claim 1, wherein the printer includes an embedded processor, and wherein the embedded processor is used to perform the decryption.

6. The method of claim 1, further comprising the step of ordering the document prior to establishing the printer identity.

7. The method of claim 6, wherein the printer is used to order the document.

8. The method of claim 6, further comprising the step of previewing at least one low quality document prior to ordering the document.

9. The method of claim 1, further comprising the step of using at least one cryptographic key to authenticate the printer prior to ordering the document.

10. The method of claim 1, wherein the printer is used to render the decrypted document.

11. The method of claim 1, further comprising the step of using the printer to indicate status of the printing so that the server can charge for copies that were actually printed.

12. A system for the distributed printing of documents, the system comprising:

a computer network;

5 a server connected to the network, the documents being stored on the server;

a printer connected to the network, the printer being programmed to use at least one cryptographic key to establish an identity with the server via the network;

10 the server being programmed to send at least one encrypted document to the printer after a document order has been placed;

the printer being further programmed to retrieve the encrypted document, decrypt the retrieved document, and print the decrypted document according to the document order.

13. The system of claim 12, further comprising a client for placing the document order.

14. The system of claim 13, wherein the server stores low quality documents for customer preview.

15. The system of claim 12, further comprising a smart card for providing at least one cryptographic key to the printer and for performing the decryption, the smart card passing the decrypted document to the printer.

16. The system of claim 12, further comprising a smart card for providing at least one cryptographic key to the printer; and wherein the printer includes an embedded processor for using at least one cryptographic key to perform the decryption.

17. The system of claim 12, wherein the printer is further programmed to indicate status of the printing so that the server can charge for copies that were actually printed.

- 5 ~~18.~~ A network printer comprising:
- means for reading at least one decryption key;
 - means for receiving an encrypted token from the remote site;
 - means for using a decryption key to decrypt the token;
 - means for send the decrypted token to the remote site;
 - means for receiving an encrypted document from the network;
 - means for using a decryption key to decrypt the document; and
 - means for printing the decrypted document.

- ~~19.~~ A network printer comprising:

a smart card reader;
a network interface;
a processor; and

- 5 memory for storing a program that, when executed, causes the processor to use the smart card reader to read a cryptographic key, use the network interface to receive an encrypted document, use the decryption key to decrypt the encrypted document, and print the decrypted document.

20. The printer of claim 19, further comprising a keypad and display; wherein the program further causes the processor to receive a document order from the keypad.

21. The printer of claim 19, wherein the program further causes the processor to send printing status to the network interface.

22. The printer of claim 19, wherein the program further causes the processor to parse a message from the decrypted document, the message indicating a number of ordered copies, and wherein the program further causes the processor to print the ordered number of copies of the decrypted
5 document.

23. The printer of claim 19, wherein the program further causes the processor to render the decrypted document.

A SECURE NETWORK-BASED SYSTEM FOR THE DISTRIBUTED PRINTING OF DOCUMENTS

ABSTRACT OF THE DISCLOSURE

An Internet-based printing system allows for the distribution and printing of documents and images in a secure, controlled manner. The system includes a secure printer that receives, decrypts and prints documents
5 supplied by a document server. Security of the system is realized by an aggregate of a secure communication protocol, smart card technology and the computational infeasibility of breaking a public key cryptographic system. The system may be used for electronic commerce, in which copies are made on a "pay-per-print" basis.

FIG. 1

FIG. 2

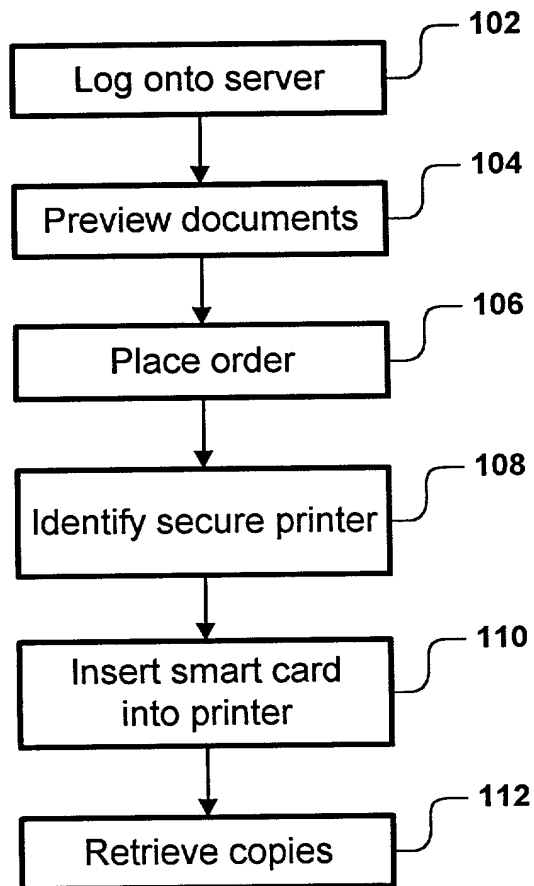
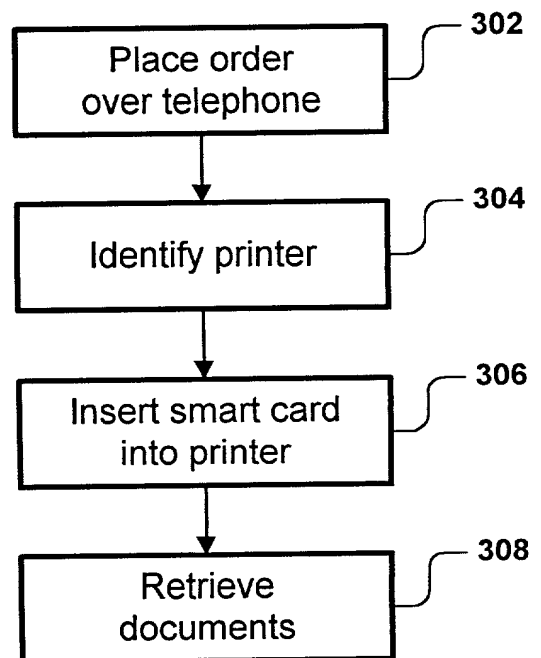


FIG. 4



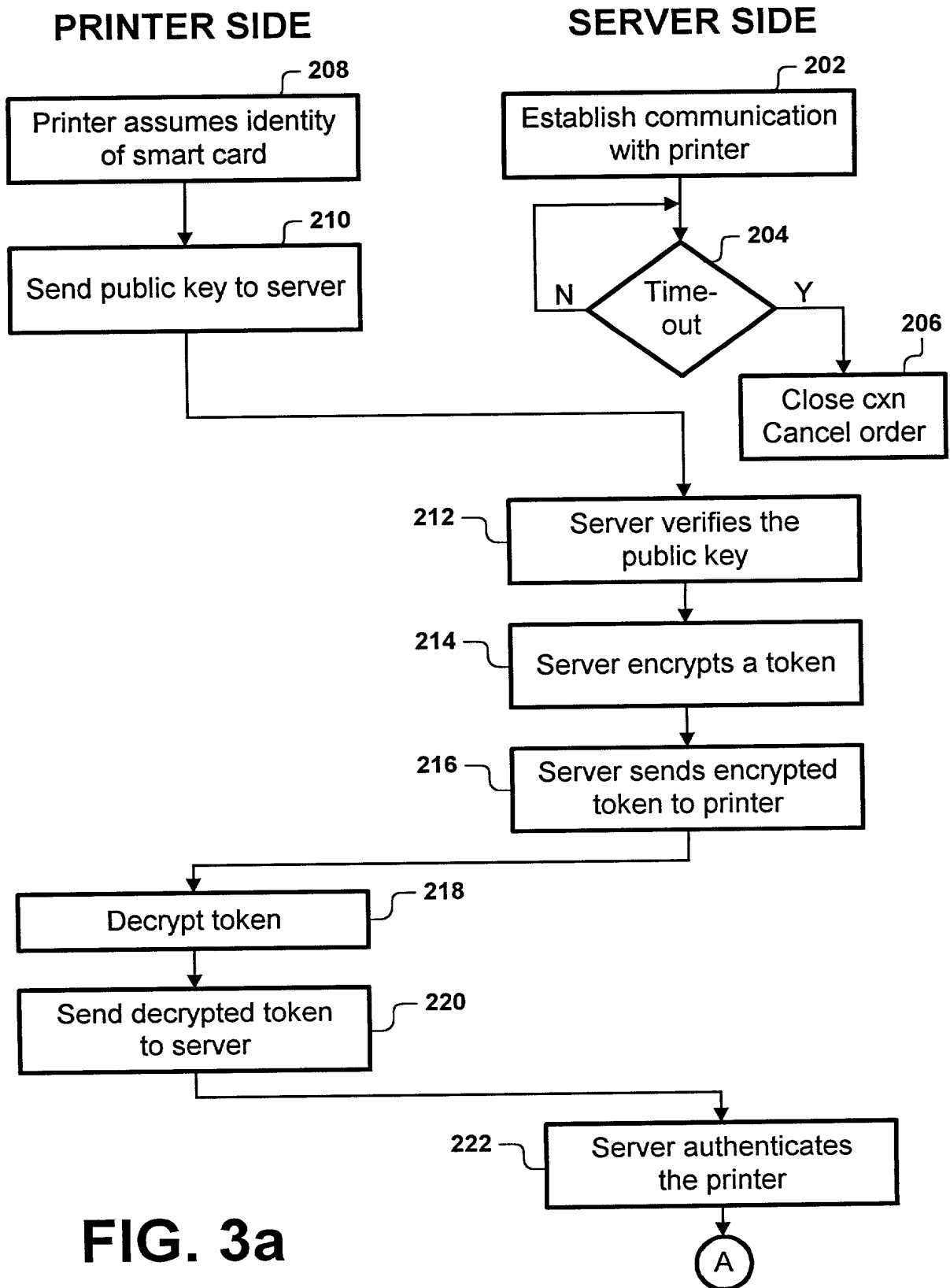


FIG. 3a

PRINTER SIDE

SERVER SIDE

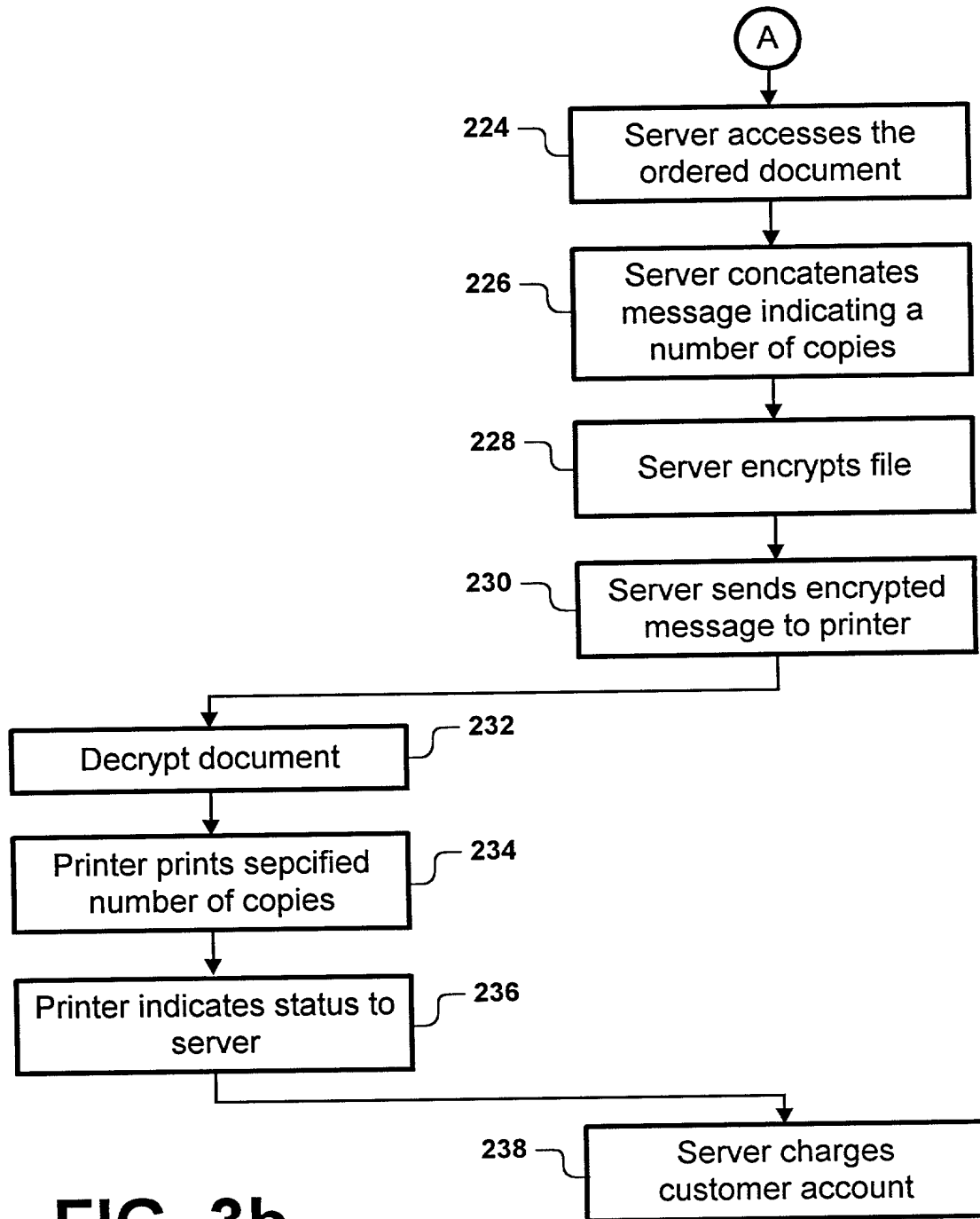


FIG. 3b

FIG. 5

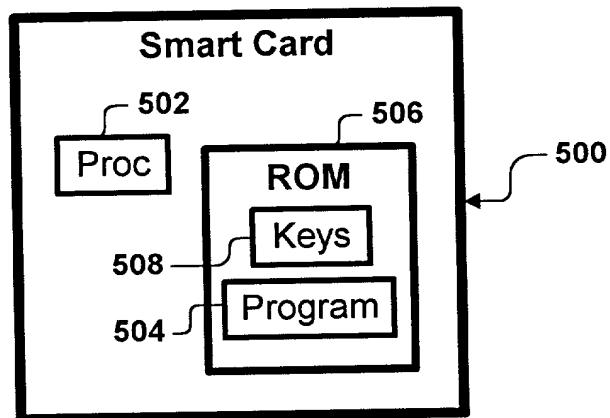
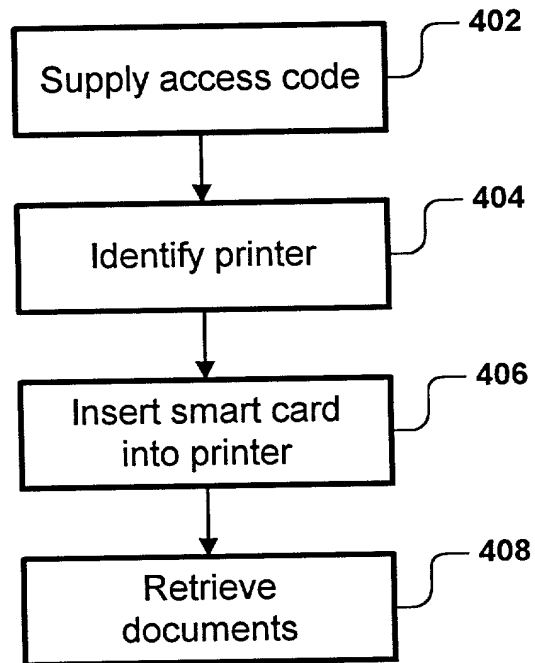


FIG. 6

DECLARATION AND POWER OF ATTORNEY
FOR PATENT APPLICATIONATTORNEY DOCKET NO. 10980251-1

As a below named inventor, I hereby declare that:

My residence/post office address and citizenship are as stated below next to my name;

I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled:

A Secure Network-Based System for the Distributed Printing of Documents

the specification of which is attached hereto unless the following box is checked:

() was filed on _____ as US Application Serial No. or PCT International Application Number _____ and was amended on _____ (if applicable).

I hereby state that I have reviewed and understood the contents of the above-identified specification, including the claims, as amended by any amendment(s) referred to above. I acknowledge the duty to disclose all information which is material to patentability as defined in 37 CFR 1.56.

Foreign Application(s) and/or Claim of Foreign Priority

I hereby claim foreign priority benefits under Title 35, United States Code Section 119 of any foreign application(s) for patent or inventor(s) certificate listed below and have also identified below any foreign application for patent or inventor(s) certificate having a filing date before that of the application on which priority is claimed:

COUNTRY	APPLICATION NUMBER	DATE FILED	PRIORITY CLAIMED UNDER 35 U.S.C. 119
			YES: _____ NO: _____
			YES: _____ NO: _____

Provisional Application

I hereby claim the benefit under Title 35, United States Code Section 119(e) of any United States provisional application(s) listed below:

APPLICATION SERIAL NUMBER	FILING DATE

U. S. Priority Claim

I hereby claim the benefit under Title 35, United States Code, Section 120 of any United States application(s) listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States application in the manner provided by the first paragraph of Title 35, United States Code Section 112, I acknowledge the duty to disclose material information as defined in Title 37, Code of Federal Regulations, Section 1.56(a) which occurred between the filing date of the prior application and the national or PCT international filing date of this application:

APPLICATION SERIAL NUMBER	FILING DATE	STATUS (patented/pending/abandoned)

POWER OF ATTORNEY:

As a named inventor, I hereby appoint the following attorney(s) and/or agent(s) listed below to prosecute this application and transact all business in the Patent and Trademark Office connected therewith.

Timothy Rex Croll

Thomas X. Li

Trueman H. Denny III

Edward Y. Wong

Reg. No. 36,771

Reg. No. 37,079

Reg. No. P44,652

Reg. No. 29,879

Send Correspondence to:
 IP Administration
 Legal Department, 20BN
 HEWLETT-PACKARD COMPANY
 P.O. Box 10301
 Palo Alto, California 94303-0890

Direct Telephone Calls To:

Timothy Rex Croll
 (650) 857-4881

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

Full Name of Inventor: Daniel R. TretterCitizenship: US

Residence:

1990 Latham Street, #18, Mtn. View, CA 94040 3085 Middlefield Rd #18, Palo AltoPost Office Address: Same as Residence

Daniel R Tretter
 Inventor's Signature

18 Nov 99
 Date

**DECLARATION AND POWER OF ATTORNEY
FOR PATENT APPLICATION (continued)**

ATTORNEY DOCKET NO. 10980251-1

Full Name of # 2 joint inventor: Thomas D. Kite Citizenship: UK

Residence: 7545 SW Hall Blvd., #29, Beaverton, OR 97008

Post Office Address: Same as Residence

Inventor's Signature: Thomas D. Kite Date: 11.29.99

Full Name of # 3 joint inventor: Qian Lin Citizenship: CN

Residence: 159 Gilbert Avenue, Santa Clara, CA 95051

Post Office Address: Same as Residence

Inventor's Signature _____ Date _____

Full Name of # 4 joint inventor: Hugh P. Nguyen Citizenship: US

Residence: 5536 Oak Park Drive, San Jose, CA 95129

Post Office Address: Same as Residence

Inventor's Signature _____ Date _____

Full Name of # 5 joint inventor: Ping Wah Wong Citizenship: Hong Kong

Residence: 1443 Knowlton Drive, Sunnyvale, CA 94087

Post Office Address: Sunnyvale, CA 94087

Inventor's Signature _____ Date _____

Full Name of # 6 joint inventor: _____ Citizenship: _____

Residence: _____

Post Office Address: _____

Inventor's Signature _____ Date _____

Full Name of # 7 joint inventor: _____ Citizenship: _____

Residence: _____

Post Office Address: _____

Inventor's Signature _____ Date _____

Full Name of # 8 joint inventor: _____ Citizenship: _____

Residence: _____

Post Office Address: _____

Inventor's Signature _____ Date _____

DECLARATION AND POWER OF ATTORNEY
FOR PATENT APPLICATION (continued)

ATTORNEY DOCKET NO. 10980251-1

Full Name of # 2 joint inventor: Thomas D. Kite Citizenship: UK
Residence: 7545 SW Hall Blvd., #29, Beaverton, OR 97008
Post Office Address: Same as Residence
Inventor's Signature _____ Date _____

Full Name of # 3 joint inventor: Qian Lin Citizenship: CN US
Residence: 159 Gilbert Avenue, Santa Clara, CA 95051
Post Office Address: Same as Residence
Inventor's Signature Qian Lin Date 11/17/99

Full Name of # 4 joint inventor: Hugh P. Nguyen Citizenship: US
Residence: 5536 Oak Park Drive, San Jose, CA 95129
Post Office Address: Same as Residence
Inventor's Signature _____ Date _____

Full Name of # 5 joint inventor: Ping Wah Wong Citizenship: Hong Kong
Residence: 1443 Knowlton Drive, Sunnyvale, CA 94087
Post Office Address: Sunnyvale, CA 94087
Inventor's Signature _____ Date _____

Full Name of # 6 joint inventor: _____ Citizenship: _____
Residence: _____
Post Office Address: _____
Inventor's Signature _____ Date _____

Full Name of # 7 joint inventor: _____ Citizenship: _____
Residence: _____
Post Office Address: _____
Inventor's Signature _____ Date _____

Full Name of # 8 joint inventor: _____ Citizenship: _____
Residence: _____
Post Office Address: _____
Inventor's Signature _____ Date _____

**DECLARATION AND POWER OF ATTORNEY
FOR PATENT APPLICATION (continued)**

ATTORNEY DOCKET NO. 10980251-1

Full Name of # 2 joint inventor: Thomas D. Kite Citizenship: UK

Residence: 7545 SW Hall Blvd., #29, Beaverton, OR 97008

Post Office Address: Same as Residence

Inventor's Signature _____ Date _____

Full Name of # 3 joint inventor: Qian Lin Citizenship: CN

Residence: 159 Gilbert Avenue, Santa Clara, CA 95051

Post Office Address: Same as Residence

Inventor's Signature _____ Date _____

Full Name of # 4 joint inventor: Hugh P. Nguyen Citizenship: US

Residence: 5536 Oak Park Drive, San Jose, CA 95129

Post Office Address: Same as Residence

Inventor's Signature Hugh P. Nguyen Date 11/24/1999

Full Name of # 5 joint inventor: Ping Wah Wong Citizenship: Hong Kong

Residence: 1443 Knowlton Drive, Sunnyvale, CA 94087

Post Office Address: Sunnyvale, CA 94087

Inventor's Signature _____ Date _____

Full Name of # 6 joint inventor: _____ Citizenship: _____

Residence: _____

Post Office Address: _____

Inventor's Signature _____ Date _____

Full Name of # 7 joint inventor: _____ Citizenship: _____

Residence: _____

Post Office Address: _____

Inventor's Signature _____ Date _____

Full Name of # 8 joint inventor: _____ Citizenship: _____

Residence: _____

Post Office Address: _____

Inventor's Signature _____ Date _____

**DECLARATION AND POWER OF ATTORNEY
FOR PATENT APPLICATION (continued)**

ATTORNEY DOCKET NO. 10980251-1

Full Name of # 2 joint inventor: Thomas D. Kite Citizenship: UK

Residence: 7545 SW Hall Blvd., #29, Beaverton, OR 97008

Post Office Address: Same as Residence

Inventor's Signature _____ Date _____

Full Name of # 3 joint inventor: Qian Lin Citizenship: CN

Residence: 159 Gilbert Avenue, Santa Clara, CA 95051

Post Office Address: Same as Residence

Inventor's Signature _____ Date _____

Full Name of # 4 joint inventor: Hugh P. Nguyen Citizenship: US

Residence: 5536 Oak Park Drive, San Jose, CA 95129

Post Office Address: Same as Residence

Inventor's Signature _____ Date _____

Full Name of # 5 joint inventor: Ping Wah Wong Citizenship: Hong Kong

Residence: 1443 Knowlton Drive, Sunnyvale, CA 94087

Post Office Address: Sunnyvale, CA 94087

Inventor's Signature Ping Wah Wong Date 11-30-88

Full Name of # 6 joint inventor: _____ Citizenship: _____

Residence: _____

Post Office Address: _____

Inventor's Signature _____ Date _____

Full Name of # 7 joint inventor: _____ Citizenship: _____

Residence: _____

Post Office Address: _____

Inventor's Signature _____ Date _____

Full Name of # 8 joint inventor: _____ Citizenship: _____

Residence: _____

Post Office Address: _____

Inventor's Signature _____ Date _____